

Ex: $x^{223} \equiv 91 \pmod{23}$

$$4 \cdot 23 = 92 \Rightarrow 91 \equiv -1 \pmod{23}$$

$$x^{223} \equiv -1 \pmod{23}.$$

Fermat's Little Thm: $a^{22} \equiv 1 \pmod{23}$

$$223 = 10 \cdot 22 + 3$$

$$\begin{aligned} -1 &\equiv x^{223} = x^{10 \cdot 22 + 3} = (x^{22})^{10} \cdot x^3 \\ &\quad \downarrow \\ &\equiv (1)^{10} \cdot x^3 = x^3 \pmod{23} \end{aligned}$$

This means:

$$-1 \equiv x^3 \pmod{23}$$

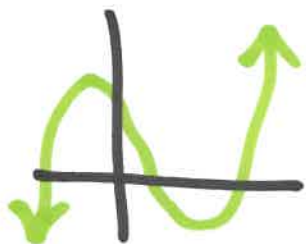
(69)

$$x^3 \equiv -1 \pmod{23}$$

$$x^3 = -1 \quad x = -1$$

This works in $\mathbb{Z}_{23}$ as well.

$x \equiv -1 \equiv 22$ is a sol.



We have a function $x \mapsto x^3$. ~~FLT~~ ~~FLT~~

$$a^{23} \equiv a \pmod{23}.$$

x	x^3	
0	0	0
1	1	1
2	8	2
3	4	3
...	...	...
22	22	22

Does $0, 1, \dots, 22$ appear in 2nd col.?

We want to undo the 3 (mod 22):

$$3^{-1} \equiv ? \pmod{22}$$

$$3^{-1} \equiv 15 \pmod{22}$$

$$x \mapsto x^3$$



$$y \mapsto y^{15} \quad z \mapsto z^3 \mapsto (z^3)^{15} \equiv z^{45} \equiv z^{15}$$

$$z^{45} = z^{22+23} = z^{22} \cdot z^{23} \equiv 1 \cdot z = z \quad (23)$$

$$z^{2 \cdot 22 + 1}$$

$$z \mapsto z^3 \mapsto (z^3)^{15} = z$$

The cube: $x \mapsto x^3$ has an inverse $y \mapsto y^{15}$.

Therefore, every number in $\{0, 1, \dots, 22\}$ must appear in 2nd col. In other words

$$x \equiv -1 \quad (23)$$

is the unique solution.

Work toward generalizing FLT and to cryptography.

Multiplicative inverses play important role.

Def. Let $m \in \mathbb{N}$. Euler's phi-function or totient function is

$$\varphi(m) = \phi(m) = |\{x \in \mathbb{Z}_m \mid \gcd(x, m) = 1\}|$$

Thus $\phi(m)$ counts the number of M.I. in $\mathbb{Z}_m$.

Ex: $m=6$

$$\mathbb{Z}_6 = \{\cancel{0}, \cancel{1}, \cancel{2}, \cancel{3}, \cancel{4}, 5\}.$$

The M.I.s are $\{1, 5\} \equiv \{1, -1\}$.

$$\phi(6) = 2.$$

Ex: $m=10$.

$$\text{M.I.s} = \{1, 3, 7, 9\}.$$

Throw out evens
and mults. of 5.

$$\phi(10) = 4.$$

Ex: $m=p$ (prime)

All ^{non-zero}
~~positive~~

$$x \in \mathbb{Z}_p$$

$$\gcd(a, p) \in \{1, p\}$$

are M.I.s

$$\phi(p) = p-1.$$

(73)

Two facts about Euler's ϕ :

① Multiplicativity. Suppose $a, b \in \mathbb{N}$ and $\gcd(a, b) = 1$.

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b).$$

② Prime powers. Let p be prime $e \in \mathbb{N}$

$$\phi(p^e) = p^{e-1}(p-1).$$

Note: $\phi(p^1) = p^{1-1} \cdot (p-1).$

Let $m \in \mathbb{N}$. By the Fund. of Arith.

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_r^{e_r}$$

p_i pair-wise
distinct

$$\phi(m) = \phi(p_1^{e_1} p_2^{e_2} \dots p_r^{e_r})$$

$$= \phi(p_1^{e_1}) \dots \phi(p_r^{e_r})$$

$$\rightarrow = p_1^{e_1-1}(p_1-1) \dots p_r^{e_r-1}(p_r-1)$$

$$= m p_1^{-1} p_2^{-1} \dots p_r^{-1} (p_1-1) \dots (p_r-1)$$

$$\rightarrow = m \cdot \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

(75)

Ex: ~~$\phi(72)$~~ $\phi(72) = \phi(8 \cdot 9)$
 $= \phi(8) \cdot \phi(9)$
 $= 4 \cdot 6 = 24.$

Ex: $\phi(26) = (2-1) \cdot (13-1) = 12.$

Thm. (Euler's Totient Thm)

If $\gcd(a, m) = 1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

$$a^{\phi(m)+1} \equiv a \pmod{m}$$

This generalizes FLT. (76)